US Army Human Resource Command Information Systems Use/Security Awareness Agreement

This agreement provides an overview of policies that apply to the use of HRC Information Systems:

1. General:

a. HRC Information Systems are available to facilitate the operational and administrative work of authorized users. These systems will be used for official government business only except for specifically authorized limited personal use IAW the Joint Ethics Regulation and will not be used for any illegitimate or fraudulent purpose. System access is not anonymous and your use constitutes consent to monitoring.

b. Users will use HRC resources responsibly and abide by normal standards of professional and personal courtesy and conduct at all times. In accessing these systems, all users agree to comply with all policies and procedures governing the use of HRC owned or supported systems. They agree to take full responsibility for all actions performed via the account assigned. Inappropriate use of these systems may be a basis for consideration of criminal or administrative disciplinary action against users. Any user who fails to comply with HRC rules and procedures will be denied system access.

c. Your Information Assurance Security Officer (IASO) is required to have you read and sign this statement and maintain it on file.

d. All users will be part of a security training and awareness program IAW Chapter 3-2, Army Regulation (AR) 25-2. The program will ensure that all users are aware of proper operational and security-related procedures and risks.

2. Environment:

a. HRC systems operate in a shared/limited resource environment processing sensitive data. As an authorized user, you have access to computer resources to do you job. Take advantage of the vast knowledge and information available through these systems to accomplish your mission, but use these resources judiciously in order to conserve our limited capabilities. Do not abuse your access.

b. HRC computer systems process defense information at the Sensitive but Unclassified (SBU) level. Information labeled SBU must be protected to ensure confidentiality, availability and integrity and may or may not require protection from foreign intelligence services or other unauthorized personnel. Examples may include information dealing with logistics, medical care, personnel management, Privacy Act data, contractual data, Freedom of Information Act information, For Official Use Only (FOUO) information and certain categories of financial data.

3.Individual guidelines:

a. Your job assignment requires your receipt of a logon ID and password that permits access to HRC information systems. Do not disclose this to anyone unless required by systems administrator, in which case you will change it afterwards. You are personally responsible for any use of your account accessed with this password.

b. Avoid any communication that could result in the disclosure of sensitive information received from HRC systems to unauthorized personnel. Information accessed will be used for official business only and disseminated only to personnel with a need to know.

c. Do not use HRC systems in a way that will interfere with your official duties, undermine readiness or reflected adversely on DOD or the Army. Your use not involve: pornography, offensive material, chain letters, unofficial advertising, personal commercial purpose or gain, soliciting, selling, game playing, illegal activities, unauthorized system access, subterfuge (using someone else's account and/or create deception as if they're responsible), inappropriately handled classified materials or other uses incompatible with public service

d. Resources will not be used in a manner that overburdens our communications systems or interferes with their performance. Do not send E-mail or make file transfers that could reasonably be expected to either cause, directly or indirectly, excessive strain on any communication facilities or unwarranted or unsolicited interference with others' use of systems.

e. Make yourself aware of and abide by the limitation and/or proper use rules for any interconnected network which you access through your account. Do not use directories other that your own, including system directories, to store files without the permission of the owner.

f. Any software on HRC systems will be legally installed and documented IAS copyright laws. Do not run any unauthorized software under your account.

g. Report any suspicious activity or erratic behavior of your system to you IASO.

4.Conscientious use of HRC systems will help avoid overburdening our scarce resources and eliminate service disruptions that could be easily avoided.

I have read the US Army Human Resource Command Information Systems Use/Security Awareness Agreement. I understand my responsibilities and I understand that my use of the system is subject to monitoring. I am accountable and responsible for my actions or actions performed by others using my account and/or privileges. If I fail to comply with the rules and procedures of this agreement, my access will be revoked and I could face criminal or administrative disciplinary action for any inappropriate use.

USER'S NAME (PRINT)	SIGNATURE	DATE

USER'S PHONE #	USER'S UNIT/SECTION/OFFICE SYMBOL

PERnet SECURITY AWARENESS BRIEFING

1. You have been assigned duties involving the use of the PERnet computer system which processes sensitive defense information at the unclassified sensitive two (US2) level. IAW Army Regulation 25-2, 14 November 2003 and is defined as follows:

US2 is unclassified information which primarily must be protected to ensure its availability, integrity and confidentiality. Such information may include logistics, medical care, personnel management, privacy act data, contractual date, and 'For Official Use Only' (FOUO) information.

2. All persons accessing an Automated Information System (AIS) will be part of a security training and awareness program IAW AR 25-2. The program will ensure that all persons responsible for managing AIS resources or who access and AIS are aware of proper operational and security-related procedures and risks. Your Information Assurance Security Officer (IASO) is required to have you read and sign this statement, and maintain it on file along with your access request.

3. Your job assignment requires receipt of logon and password that permits access to a computer system processing sensitive information. You must bear in mind that AR 25-2 requires all such password to be controlled at the highest level if sensitive information is on the system.

4. I (supervisor) am required to impress upon you the extreme need for caution and discretion in any contracts, either personal or professional. As in any interesting activity, the temptation is great to refer to your professional accomplishments. You are cautioned to avoid any conversation that could result in a disclosure of sensitive information received from PERnet systems to unauthorized personnel.

5. Personnel failing to comply with the rules and procedures of this activity will have their access revoked.

I have read the PERnet System Usage Agreement and the PERnet Security Awareness Briefing and understand my responsibilities.

USER'S SIGNATURE	DATE
SUPERVISOR'S SIGNATURE	DATE

INSTRUCTIONS FOR COMPLETING TAPC FORM 49-R

All blocks must be filled out legibly and completely in accordance with these instructions. Failure to comply will delay or prevent the processing of your request.

TASO / IASO must submit completed forms to the PERNET Registrar: at userregistrar@hoffman.army.mil or debra.trimble@hoffman.army.mil . Scanned copies are preferred over faxed copies as they provide a better quality of resolution.

Block #	INSTRUCTIONS
1	Self-explanatory
2	Military or Civilian GS rating
3	Select appropriate block
4	Enter your room number
5	List same organization as the TASO's organization on the TAPC Form 50-R
6	List same Office Symbol as the TASO's office symbol on the TAPC Form 50-R
7	a-c: List duty address as requested
8	a-b: List duty phone number as requested
9	Be specific with duty title (i.e. Records clerk/MPD, Promotions clerk, etc)
10	List units Major Command (i.e. FORSCOM, IMA, USAREUR)
11	If user has a PERNET account check "Update": If no current account check "New"
12	Check "NO" and list requester's arrival date to organization
13	If user already has a PERNET Account list the account # here (user's account number is on their previous TAPC-R form in block 30)
14	List PERNET ID for those with current accounts (must have checked "Update" in block # 11.
15	Leave blank
16	List all access being requested: If user is requesting a TOPMIS II Account, have them put "CITRIX" under block 14a (Other). Request for DATAQUERY Accounts must be accompanied by a separate memorandum of justification. Generally, only those working in the PAS should have DQ access due to its complicated nature. MUST INCLUDE AKO USER ID.
17-20	List information of TASO / IASO (name must match that on file with PERNET Security). Must include all pertinent information or accounts will not be established
21	Have unit Security manager check this block. A favorable NAC Background check is required for access --- this is not the same as a SECRET Clearance. Requestor does not need to have a SECRET clearance for access to PERNET
22-24	Have Security manager complete all blocks and sign / date in the appropriate blocks
PART C	Brief the user on the HRC Information Systems Use / Security Agreement and maintain on file with the Requestor's application.

Submit completed application to: PERNET REGISTRAR at above email

PERnet SYSTEM ACCESS REGISTRATION

A. USER/IASO INFORMATION

Date:

1. USER NAME (Last, First, Middle Initial)	2. Grade	3. Employee Type: ☐ Govt ☐ Contractor	4. Room# / Mail Stop:

5. Organization/Contractor Company:	6. Office Symbol:

7. Address a. Street:	b. City/State:	c. ZIP Code:

8. User Phone Number:	DSN:	COMM:

9. Duty/Position Title:	10. MACOM/ARQODA:

11. Type of Request:	New	Update	Transfer	Delete

12. Pre-Registration: (ORB/2A, Attached)	Yes	No	Arrival Date:

13. Transfer From Acct #:	14. PERnet Userid:

15. Access Requested:	TOPMIS II		EDAS		MS51		COPS		DCIPS		DATA QUERY	

OTHER	a:	b:	c:	d:	e:

f: AKO User ID: _____@us.army.mil

16. IASO Name:	17. Signature:

18. IASO Phone Number:	DSN:	COMM:	FAX:

19. Account Number (if known) :	20. IASO AKO:

PART B. SECURITY INVESTIGATION STATUS (TO BE COMPLETED BY SECURITY MANAGER)

21. **"I verify that a favorable National Agency Check (NAC) or a favorably adjudicated NAC investigation has been completed on the user. I will notify the IASO who in turn will notify ISD Security immediately to terminate this access approval if the investigation status of the user changes"**

☐ **I Verify**

"HRC Users Only - If the access requested is for a classified system, I verify the user has a valid SECRET clearance. If the person holds an ADP I position as specified in AR 380-67, I verify that a successful Single Scope Background Investigation has been completed"

☐ **I Verify**

22. Security Manager's Name:		

23. Phone Number:	DSN :	COMM:

24. Signature:	Date:

PART C. IASO CERTIFICATION

I, _____ **have briefed/will brief** _____
on the AHRC Form 49-1-R (AHRC Information System Use/Security Awareness Agreement). I will maintain the signed copy on file along with access information.

PART D. FOR PERSINSD USE ONLY

25. PERnet Userid:	26. CICS Opr ID:	27. Company Code:	28. Org. Code:

29. SIC Code:	30. Account Number:

31. ISD Security/Phone/Date:	32. Remarks:

33. Domain User ID:	34. Legacy User ID